跡見学園女子大学マネジメント学部紀要　第 34 号　2022 年 8 月 5 日

# サイバー犯罪の現状と課題

## ――デジタル・フォレンジックに注目して――

## Current Situation and Issues on Cybercrime —Focus on digital forensics—

深　町　浩　祥
Hiroyoshi FUKAMACHI

**要　旨**

本稿は、近時のサイバー犯罪における現状と課題を、法的紛争・訴訟に対処するための一連の科学的調査手法・技術であるデジタル・フォレンジックに注目して考察するものである。近時のサイバー空間の脅威としては、新しいサービスや技術を悪用した犯罪の発生があげられる。国内では、ランサムウェアよる被害件数の増加や不正アクセスによる情報流出、国家を背景に持つサイバー攻撃集団の存在が明らかになるなど、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いている。このような重大サイバー犯罪に対処するため令和 4 年 4 月 1 日に改正警察法が施行され、サイバー警察局やサイバー特別捜査隊が設置されることとなった。

サイバー犯罪の証拠保全と分析には、デジタル・フォレンジックの手法が用いられ、その証拠能力は訴訟等において重要な要素となってきている。しかし、サイバー空間の犯罪者の技術的能力は高く、電磁的記録に痕跡データを残さない場合も多いことや、ICT 技術のプライバシー保護の技術が逆に作用し、犯罪者の特定は困難になっていることが明らかとなった。さらに、デジタル・フォレンジックの手続き過程での物理コピーや情報収集・解析に関連して著作権やプライバシー保護に関する法的課題があること、また、改正警察法に対する期待と懸念があることを示した。

**キーワード**：サイバー犯罪、電磁的記録、デジタル・フォレンジック

## はじめに

本稿の目的は、今日のサイバー犯罪の現状と課題を、法的紛争・訴訟に対処するための一連の科学的調査手法・技術であるデジタル・フォレンジックに注目して考察するものである。

我が国の刑法犯の認知件数は平成 14（2002）年を最多として、その後約 20 年にわたり減少を続けている[1]。その一方で、サイバー犯罪は統計的には増減を繰り返しつつも増加傾向にあり、その深刻さを増している。今日のサイバー犯罪は、特定のコミュニティや地域、国内だけではなく国際的な重要課題となっている[2]。我が国でも深刻化する海外からのサイバー攻撃は摘発が難しく、令和 4（2022）年 4 月 1 日施行の改正警察法により警察庁はサイバー警察局を新設し、国際捜査へ積極的に参加し摘発に向けて準備を進めている[3]。

サイバー犯罪には、電磁的記録[4]の不正利用（なりすまし等）[5]によるもの、ソーシャルネットワーク（SNS）での誹謗中傷による事件[6]などのような個人の信用棄損を伴うもの、非常に感染力・拡散力が強いマルウェアのエモテット[7]、ランサムウェアによる攻撃[8]により官公庁[9]や企業[10]、大学[11]などの機能を停止させるようなもの、などがある[12]。

サイバー犯罪においては、被害者を保護し、犯人を特定するための情報技術などの含めた学際

---

1　法務総合研究所編（2021）『令和 3 年版犯罪白書』法務省、3 頁。https://www.moj.go.jp/content/001365724.pdf（2022.2.22 閲覧）

2　特殊詐欺，児童虐待，配偶者間暴力，サイバー犯罪等のように検挙件数が増加傾向または高止まり状態にある犯罪もある。法務総合研究所編（2021）『令和 3 年版犯罪白書』法務省　はしがき。https://www.moj.go.jp/content/001365724.pdf（2022.2.22 閲覧）

3　『警察法の一部を改正する法律案』警察庁 https://www.npa.go.jp/laws/kokkai/220128/03_sinkyu.pdf（2022.04.02 閲覧）

4　法は電磁的記録について、「電子的方式、磁気的方式、その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの」（刑法 7 条の 2、民事訴訟法 3 条の 7 第 3 項カッコ書）とする。しかし、1987 年刑法改正により当該概念が導入された際の立案者の解釈に過ぎない。一般に、電磁的記録とは情報が「記録、保存されている状態」を表す概念とされる。渡邊卓也（2018）『ネットワーク犯罪と刑法理論』成文堂、103 頁。

5　「メールなりすまし攻撃　日本企業の約 8 割が対策不備」日本経済新聞電子版　https://www.nikkei.com/article/DGXZQOUC283MG0Y2A120C2000000/（2022.2.17 閲覧）

6　「木村花さんツイッター中傷、投稿者に 129 万円賠償命令」朝日新聞デジタル　https://www.asahi.com/articles/ASP5M52KHP5MUTIL026.html（2022.2.17 閲覧）

7　警視庁「Emotet（エモテット）感染を疑ったら」https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/emotet.html（2022.3.29 閲覧）

8　「「身代金」ウイルス、国内 11 病院が被害…救急搬送や手術に支障も」読売新聞オンライン　https://www.yomiuri.co.jp/national/20211228-OYT1T50173/（2022.2.17 閲覧）

9　「内閣官房のデータ流出 サイバー攻撃対応の訓練情報も流出判明」NHK　https://www3.nhk.or.jp/news/html/20210602/k10013064581000.html（2022.2.17 閲覧）

10　「サイバー攻撃、トヨタ取引先に照準　中小の防御甘く」日本経済新聞電子版　https://www.nikkei.com/article/DGXMZO63737630R10C20A9TJ3000/（2022.2.17 閲覧）

的な知見が求められる。そして、犯人を特定するために近年注目されているのがデジタル・フォレンジックである。

デジタル・フォレンジックとは犯罪の立証のための電磁的記録の解析技術及びその手続、インシデントレスポンス[13]や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術をいう。電磁的記録を犯罪捜査や裁判証拠に利用することが求められる。犯行を未然に防ぐことが非常に難しくなっている現在のサイバー犯罪[14]においては、これまでのセキュリティ戦略からの転換が求められている。そこで、本稿ではサイバー犯罪の現状と課題を整理したうえで、その対策として行われているデジタル・フォレンジックの技術的な側面と法的な側面の課題と対応策を整理したい。

まず第1に、サイバー犯罪の特徴や類型そして近時の動向と警察庁等の対応について整理する。第2に、デジタル・フォレンジックの手順と内容について整理し、技術的な課題と対応策を検討する。第3に、デジタル・フォレンジックが利用された裁判事例等を概観した後に、デジタル・フォレンジックに関わる法的課題について整理し対応策について考察する。

## 1　サイバー犯罪の特徴・類型・動向

本章ではサイバー犯罪の特徴と現在の動向について整理する。

### 1－1　サイバー犯罪とは

サイバー犯罪の概念は、サイバー空間との関連をどこまで取るか、法律上どのような行為が犯罪とされるかによって定められる[15]。現在では、インターネットによって世界的に広がるサイバー

11 「東京大学管理の HPCI 機材への不正アクセスについて 2021.10.15」東京大学情報基盤センター https://www.itc.u-tokyo.ac.jp/blog/2021/10/15/post-3198/（2020.3.31 閲覧）

12 サイバー犯罪対策プロジェクト（2022）「令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」警察庁 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf（2022.3.20 閲覧）

13 インシデントレスポンスとは、コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等（インシデント）への対応等をいう。

14 「もう攻撃は防げない　竹中工務店の大転換」日経 BP　https://xtech.nikkei.com/atcl/nxt/mag/nc/18/080600188/080600001/（2022.2.17 閲覧）

15 中野目善則・四方光編著（2021）『サイバー犯罪対策』成文堂、3頁。

空間で敢行されることを重視してサイバー犯罪と呼ばれている。しかし、インターネットにつながっていない単体の電子機器への攻撃に関わる犯罪のことについてもサイバー犯罪の概念に含まれることが多い[16]。本稿では、プログラムだけでなく電子機器のインシデントに関わる犯罪についてもサイバー犯罪として扱うこととする。

我が国において、サイバー犯罪という言葉についての法律上の定義、あるいは学問上の通説となっている定義があるわけではない。警察庁は国民に対してサイバー犯罪の現状を知らせるための統計として計上する範囲について、①不正アクセス禁止法に規定された不正アクセス、②刑法に規定された不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪、③インターネットを主な手段とした各種の総称であるインターネット利用犯罪をもってサイバー犯罪、としている[17]。

### 1－2　サイバー犯罪の特徴

サイバー犯罪の特徴として、変化の速さ、越境性、電気通信であること、暗数（犯罪被害実態）の多さ、ICT専門性、個人情報の転売市場の存在、など6点を挙げることができる。以下では、それぞれの内容について整理したい。

**(1) 変化の速さ**：サイバー空間を具体的に構成するのは、プラットフォームやSNS等である。それらのプラットフォームやSNSなどは、通常、利用者に対するセキュリティが低いままサイバー空間に公開され、徐々にセキュリティを高めていくという過程を踏む。したがってサイバー犯罪は、プラットフォームやSNSが新規に登場して間もない期間におけるセキュリティの脆弱性を狙って行われることが多い。サイバー犯罪は、サイバー空間に新しいアプラットフォームやSNSが日々登場する速さと同じように変化するのである[18]。

日々加速する変化の中で、従来の刑事実体法では捉えられない不当行為が行われたり、従来の刑事手続法では対処できない犯罪事象が生じたりする。実際、我が国だけでなく諸外国においても、サイバー犯罪に対処するための刑事立法は、他の分野に比べて頻繁に行われている。このような現状を踏まえると、サイバー犯罪の分野においては、法律学における立法論が重要となるとともに、既存の法律の条文の本質に添った柔軟な解釈による対応の必要性も高まることとなる[19]。

---

16　中野目・四方・前掲注（15）4頁。

17　中野目・四方・前掲注（15）4頁。警察庁「令和元年におけるサイバー空間をめぐる脅威の情勢等について」（令和2年3月25日）参照 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_cyber_jousei.pdf（2022.3.22閲覧）

18　中野目・四方・前掲注（15）10頁。四方光「複雑系としてのサイバー犯罪」（2021）『法学新報127巻9・10号』1頁。

19　中野目・四方・前掲注（15）10頁。

しかし、刑事法の解釈における柔軟な対応は、罪刑法定主義[20]や強制処分法定主義[21]との関係で重大な問題を生じかねない。その一方で、刑事法の解釈によって可能かつ柔軟な対応をしないことにより、サイバー犯罪の著しい変化に伴う重大な不公正を相当期間放置することは、上記の問題を越えた不正義を生み、さらには刑事司法に対する信頼を著しく低下させることになりかねない[22]。

**(2) 越境性**：現実世界の犯罪と違い、サイバー空間は国境を自由に越える通信により構成されている。そのため、サイバー犯罪だけでなく現実世界の犯罪であっても、電磁的記録を求めようとすると、直ちに国境を越える捜査活動を要することになる。ところが、捜査権や裁判権は国家主権にあたるため、他国の領域においては証拠収集活動を行うことができないのが原則である。したがって、国境を越える捜査を行う場合には、どのような軽微な犯罪・手続であっても、何らかの国際捜査共助の手続によらなければならないのが原則となる。それをどのように円滑化するかが、我が国だけでなく国際社会においても大きな課題となっている[23]。

**(3) 電気通信としての特徴**：サイバー空間におけるあらゆる行動が電気通信として行われることに伴う特徴として、以下の３点が挙げられる。第１に、サイバー犯罪における直接の標的は、無限に複製・回復が可能で排他性のない電磁的記録としての情報であることから、現行刑法では財産犯の対象となる財物とされていない。そのため、サイバー犯罪に対しては、伝統的な刑事実体法は適用することができず、適切に規制するためには新たな犯罪として刑罰法規を新設することが必要となる[24]。第２に、現実空間の犯罪に比べて、電気通信は、非可視的なため、サイバー犯罪の存在は容易には明らかにならない。被害者ですら犯罪被害を認識できないことが多い。第３に、サイバー犯罪の捜査は、通信もしくはその記録に対する捜査となることが多く、憲法上、電気通信事業法上の通信の秘密が問題となる。したがって、現実世界であれば任意捜査とされる捜査が、サイバー犯罪においては、通信の秘密やプライバシーを侵害する強制捜査となることが頻繁に生じる。このことは、最終的には内容が公表される通信でも、公表前の通信やその記録の捜査においてもあてはまる。一方で、通信の結果としてウェブサイト上で行われる行為は、憲法上保護される表現となる。そのため、サイバー犯罪を規制する刑事実体法は、表現の自由の侵害とならないかが問題とされることが多い[25]。

---

20　罪刑法定主義とは、いかなる行為が犯罪とされ、それにいかなる刑罰が科せられるかということを、あらかじめ法律で定めておかなければ人を処罰することはできないとする近代自由主義刑法の基本原則。ドイツの刑法学者フォイエルバッハが、罪刑法定主義をはじめて明確に提唱。

21　強制処分法定主義とは、強制的な手段を使う捜査（強制捜査）は、法律に基づいてのみ行えるという立場のこと。

22　中野目・四方・前掲注（15）11頁。

23　中野目・四方・前掲注（15）11頁。

24　中野目・四方・前掲注（15）11頁。

25　中野目・四方・前掲注（15）12頁。

**(4) 暗数（犯罪被害実態）の多さ**：サイバー犯罪は、他の罪種に比べて暗数が大きいとされる。その理由は、サイバー犯罪は個々の被害が被害額僅少・犯罪軽微かつ捜査困難なため、検挙率が低く被害者が被害を届け出ない割合が高いと考えられるからである[26]。また、サイバー犯罪の中には、被害者が被害を認識できないものも多い。例えば、不正アクセスによるウイルスの感染や情報の窃取などは、被害者に気づかれないよう巧妙に行われるため、被害者が被害を認識していない場合が非常に多いと推測される[27]。また、航空会社などのように、被害を届け出たり、公表したりすることが逆に派生的に重大な問題を引き起こすような場合は、一般には認識されない可能性がある[28]。

**(5) ICT（ Information and Communication Technology）に関する専門性の必要性**：サイバー犯罪の特性に対処するための立法や政策立案、犯罪捜査や訴訟活動においては、必然的に ICT に関する専門的知識技能を要することとなる。サイバー犯罪は、高度な専門家の知見を要する社会事象であり、立法や政策の立案の際は、サイバー空間や ICT 技術に関する専門家の知見を参考にすることが重要である。そのためには、立法者や政策立案者が、専門家の知見を理解できる程度には ICT 技術を把握している必要がある[29]。この点で、法と技術に通じる学際的な人材の必要性が高まっているといえる。サイバー犯罪対策においては、立法段階、捜査段階に限らず、裁判段階においても、それに従事する担当者は、サイバー犯罪に関するある程度の学際的な専門的知識を有していなければならないと考えられる[30]。

**(6) 個人情報の転売市場（ダークマーケット）の存在**：サイバー犯罪によって、組織から違法な手段で盗まれた個人情報は、さまざまな場所で取引される。ダークウェブ[31] に存在するマーケットプレイス（以下ダークマーケット）や個人情報オークション、犯罪系コミュニティ、SNS、コミュニケーションアプリなどで取引が行われ、犯罪の連鎖を生みだす場が存在する[32]。このようなダークマーケットの存在は、上記（1）～（5）までのサイバー犯罪の特徴を包括したものということができる。

ダークマーケットへの個人情報の流れを止め、転売による再犯を防ぐための技術的な対応を行うことで、犯罪のコストを上げ、盗まれた個人情報の市場価格を下げるという観点が重要である。攻撃者の動向を継続的に調査し効果的な対策を探り続けていく必要がある[33]。

---

26　中野目・四方・前掲注（15）12 頁。

27　実際、ボットネットという多数のパソコン等をウイルスに感染させる仕組みでは、警察等が把握し、通知して初めて感染を認識する被害者が非常に多い。

28　大久保隆夫「航空分野のサイバーセキュリティと人材育成」（2020）『情報処理第 61 巻第 4 号』情報処理学会、350 頁。

29　中野目・四方・前掲注（15）13 頁。

30　中野目・四方・前掲注（15）14 頁。

31　サイバー犯罪の犯罪者が犯罪の道具を交換する場所が、ダークウェブ（dark web）である。中野目・四方・前掲注（15）6 頁。

## 1－3　サイバー犯罪の類型

サイバー犯罪は、刑法上はコンピュータ・電磁的記録に関する罪、ネットワーク利用犯罪、不正アクセス禁止法違反の3つに大きく分けられる。しかし、サイバー犯罪はICTの進歩とともにその犯罪形態が多様化している[34]。本節ではサイバー犯罪の類型について、(1) サイバー空間上の不法侵入 (2) 猥褻文書画像の頒布 (3) 匿名性を利用した言葉の暴力 (4) 詐欺等の財産犯 (5) 電子機器に対する物理攻撃、という5つの類型を整理する。

### (1) サイバー空間上の不法侵入

サイバー空間上の不法侵入の典型は、利用者のID・パスワード等によって管理されたコンピュータに対するハッキングである（不正アクセス禁止法の不正アクセス罪）。他人のID・パスワードを無断で使用する不正ログイン型と、コンピュータ制御の脆弱性を突いて侵入する脆弱性攻撃型がある。特定の標的をウイルスに感染させることを目的に、当該標的の知人になりすましたメールを送付する標的型メール攻撃[35]やD-Dos攻撃[36]、ランサムウェア[37]も、この類型として論じられる[38]。

各種のウイルスの感染のために使用されるのが、ボットネット[39]である。これは、犯罪者が多数の他人のサーバをウイルスに感染させてC & Cサーバ[40]として支配し、標的のサーバに通信を集中させたり、多数のコンピュータに偽メールを送付したりする。犯罪者は、サイバー犯罪の取締りの緩慢な国に設置された、通信記録を残さず捜査にも協力しないプロキシサーバを利用することが多い。また、世界中の数千～数万ともいわれる協力サーバを仲介して、発信元をたどれな

32　盗まれた個人情報は、データブローカーやコミュニティの共有者を通じて、多様な犯罪者コミュニティに拡散されていく。松本隆「盗まれた個人情報の市場価値―デジタル・フォレンジックに携わる現場より」(2021)『情報処理第62巻第8号』情報処理学会、e21頁。ダークマーケットの利用者にとって対価を支払う価値のある個人情報は、より深く「特定の個人になりすますための情報」だということである。市場が特定の個人にかかわる情報をとりまとめたデータであるFullz（フルズ）単体よりも運転免許証データの方が高い価値となるが、それは、具体的な悪用のしやすさにあると考えられえる。ダークマーケットで商品を購入する犯罪者は、入手したデータを活用し、自分の非合法なビジネスや活動の目的を達するために購入する。松本（2021）e22頁。

33　松本・前掲注（32）e25頁。

34　中野目・四方・前掲注（15）56頁。

35　朝日新聞デジタル「虚偽の指示で約40億円詐欺被害　トヨタ紡織欧州法人」(2019年9月10日) https://www.asahi.com/articles/ASM965H5HM96OIPE02Q.html（2022.2.22閲覧）

36　大量の情報を標的とするコンピュータに集中的に送付して機能を停止させる手口

37　指定の金額を支払わないとコンピュータの機能を停止したままにすると脅す企業恐喝に使用される。

38　日本経済新聞電子版「ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃」(2021年11月12日) https://www.nikkei.com/article/DGXZQOUE071OK0X01C21A1000000/（2022.2.22閲覧）

39　ボットとは、ウイルスに感染させて支配下においたロボットの意味。

40　Command and Control server：ボットネットに指令を送信制御するサーバ。

い技術を用いたネットワークである Tor（The Onion Rooting）も構築されている[41]。

**(2) 猥褻文書画像の頒布**

サイバー空間上の猥褻文書の典型は、文字通り猥褻文書のウェブ上の公開、販売、広告である。インターネットは、画像の頒布において現実空間とは比較にならない力を発揮する。児童ポルノは、今日では、猥褻文書というより、児童の性的虐待の記録として扱われることが多い。リベンジポルノや SNS の売買春の誘引は、海外でも問題となっている[42]。

**(3) 匿名性を利用した言葉の暴力**

サイバー空間上の暴力とは、インターネットで展開される言葉の暴力のことである。技術力のあるハッカーではなく、匿名性を背景に、普通のインターネット・ユーザーが過激な言動を行う。日本で問題になっているネットいじめ、インターネットを用いたストーカー行為、炎上、ヘイトスピーチ、ネット上の名誉棄損が、海外でも問題となっている[43]。

**(4) 詐欺等の財産犯**

詐欺等の財産犯としては、架空の取引により代金や商品を詐取するインターネット詐欺、財産の隠匿を企図する大富豪を名乗って巨額の謝礼を支払う代わりに当面必要な資金の提供を求めるナイジェリア詐欺、インターネットを通じて相手に恋愛感情を持たせて金品を要求するロマンス詐欺、暗号資産への投資を名目とした詐欺、インターネットを利用した著作権侵害など、日本でも海外でも見られる犯罪がある。技術力のない者であってもノウハウの教示を受けて敢行することができる財産犯であり、潜在的な犯罪者の数は多いものと考えられ、今後の広がりが懸念される[44]。

**(5) 電子機器に対する物理攻撃**

近年、IoT（Internet of Things）やサイバーフィジカルシステム（Cyber Physical system ）が重要となってきている。このようなシステムをサイバー犯罪から守るためには、プログラムが動作する場である物理的な電子機器にも注目する必要がある。なぜなら、電子機器はプログラムよりも低い階層で動作するため、プログラムでは電子機器階層に対する脅威への対応が難しいからである。電子機器階層の脅威の例として、電子機器チップから漏れ出る電磁波の物理的な観測による暗号鍵の解析や、意図的な機能の停止や情報漏洩を引き起こす電子機器トロージャン、センサに対する攻撃などが報告されており、これらの電子機器階層の脅威はシステムの安全性に大きな影響を与えている[45]。

---

41　中野目・四方・前掲注（15）5-6 頁。

42　上野紫野「誹謗中傷と有害情報」（2021）『ジュリスト＃ 1554』有斐閣、38-43 頁。中野目・四方・前掲注（15）6 頁。

43　宍戸常寿「インターネット上の誹謗中傷問題」（2021）『ジュリスト＃ 1554』有斐閣、14-18 頁。曽我部真裕「匿名表現の自由」（2021）『ジュリスト＃ 1554』有斐閣、44-49 頁。

44　中野目・四方・前掲注（15）6-7 頁。

## 1－4　サイバー犯罪の動向と改正警察法

我が国の刑法犯の認知件数は、平成 8（1996）年から毎年戦後最多を更新し平成 14（2002）年には 285 万 4,061 件にまで達したが、平成 15（2003）年に減少に転じて以降、18 年連続で減少となった。そして、令和 2 年は 61 万 4,231 件（前年比 13 万 4,328 件（17.9％）減）と戦後最少を更新した[46]。令和 3（2021）年に全国の警察が検挙したサイバー犯罪が前年比 24.3％増の 1 万 2,275 件（暫定値）で過去最多となり、暗号資産（仮想通貨）に絡んだ詐欺事件などが増えた[47]。

近時のサイバー空間の脅威情勢として、サイバー空間には、新しいサービスや技術を悪用した犯罪が続々と発生している[48]。国内では、ランサムウェアよる被害件数は 146 件と増加を続けている。特に、新型コロナウイルス蔓延の対策として増加したリモートワークで、一般的なインターネット回線を利用して作られる仮想のプライベートネットワークである VPN（Virtual Private Network）のセキュリティが高いとされ普及したが、その VPN 機器の脆弱性等を狙われた被害が多くなった。また、不正アクセスによる情報流出や、国家を背景に持つサイバー攻撃集団によるサイバー攻撃が明らかになるなど、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いている[49]。

国内の医療機関においては、電子カルテ等のシステムがランサムウェアに感染し、新規の診療受付や救急患者の受入れが一時停止する事態となる[50]など、重要インフラ事業者が標的となった。令和 3（2021）年 5 月に発生した米国の石油パイプライン事業者を標的とした攻撃[51]など、ランサムウェア攻撃は、世界各国において市民生活に重大な影響を及ぼしており、その対策には、緊密な国際連携が求められている。警察では、内閣サイバーセキュリティセンター（NISC）と連

45　松本勉・佐々木貴之・石黒正輝「電子機器セキュリティの最新動向」（2020）『情報処理第 61 巻第 6 号』情報処理学会、560-563 頁。アメリカのセキュリティ機関である NIST が電子機器セキュリティのベストプラクティスの検討を開始したり、日本においても経済産業省が発行しているサイバー・フィジカル・セキュリティ対策フレームワークにおいて電子機器の信頼性が言及されたりと、電子機器セキュリティの重要性の認識が広まっている。

46　法務総合研究所編（2021）『令和 3 年版犯罪白書』法務省、3 頁。

47　サイバー犯罪対策プロジェクト（2022）「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」警察庁 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf（2022.3.20 閲覧）

48　サイバーセキュリティ政策会議「実空間とサイバー空間とが融合したデジタル社会の安全・安心の確保」（令和 3 年 12 月）（https://www.npa.go.jp/cybersecurity/CS.html）

49　サイバー犯罪対策プロジェクト（2022）「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について（速報版）」警察庁 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf（2022.3.20 閲覧）

50　前掲注（8）

51　「サイバー被害の米パイプライン、身代金 4.8 億円の支払い認める 2021.5.20」BBC NEWS｜JAPAN https://www.bbc.com/japanese/57181463（2022.3.30 閲覧）

携して、関係機関と連携した情報収集や対策等を進めていくとしている。

また、令和3（2021）年に警察庁が実施した治安に関するアンケートにおいて、サイバー犯罪の被害に遭う危険性について「不安を感じる」又は「ある程度不安を感じる」との回答が79.4%に上るなど、国民が抱く不安感も高まっている。

上記のような情況に対応するため、改正警察法が令和4（2022）年1月28日閣議決定され、第208回国会（常会）に提出、同年3月31日に可決成立し、同年4月1日より施行された。その立法趣旨は、最近におけるサイバーセキュリティに対する脅威の深刻化に鑑み、国家公安委員会及び警察庁の所掌事務に重大サイバー事案に対処するための警察の活動に関する事務等を追加するとともに、警察庁が当該活動を行う場合における広域組織犯罪等に対処するための措置に関する規定を整備するほか、警察庁の組織について、サイバー警察局を設置する等のため、とされている[52]。

改正の要点としては以下のようなものがある。まず第1に、国家公安委員会の任務（第5条第1項）達成のため、広域組織犯罪等を規定し（第5条第4項第4号）、重大サイバー事案に係る犯罪の捜査その他の重大サイバー事案に対処するための警察の活動に関すること（第5条第4項第16号）について警察庁の所掌事務を管理すると規定している。第2に、警察庁の内部部局として、旧法の情報通信局ではなくサイバー警察局を設置し（第19条）、当該局の所掌事務をサイバー事案に関する警察に関すること（第25条）とした。第3に、そのサイバー事案や技術に関わる警察活動を関東管区警察局に分掌させ（第30条の2）、関東管区警察局の管轄区域を全国とし、一元管理させることとした。第4に、都道府県警察相互間の関係について、重大サイバー事案での警察庁と各都道府県警察による共同しての処理を認め、警察庁長官が任命した警察職員に、その指揮を委ねるとした（第61条の3第3項、第4項）。また、国の機関が捜査することを受け、国家公安委員会に苦情を申し出ることができる規定を設けた（第79条第1項）。

重大サイバー犯罪への対処とサイバーセキュリティに対する脅威が深刻化する中で、警察庁は新たにサイバー警察局と重大サイバー事案について警察庁が直接捜査するサイバー特別捜査隊を設置した。デジタル社会の進展でサイバー犯罪のリスクが増す中、高度なサイバー攻撃に対応し、海外の機関と連携することを目指すこととなった。

52 「案文・理由」『警察法の一部を改正する法律案』警察庁 https://www.npa.go.jp/laws/kokkai/220128/02_anbun.pdf（2022.04.02閲覧）

## 2　デジタル・フォレンジックの手順と専門技術

サイバー犯罪に関わるインシデントが発生した際には、コンピュータなどの情報処理機器やネットワーク上に残された証拠を確保し、将来起こり得る裁判に備えるための技術や手順が必要になる。これが、本稿で対象とするデジタル・フォレンジックである。

デジタル・フォレンジックは警察などの法執行機関が使う場合もあれば民間で用いる場合もある。また、サイバー攻撃のように情報処理機器を直接の対象とする不正侵入や情報漏洩等のインシデントだけでなく、殺人事件や窃盗、談合、インサイダー取引、不正会計、契約違反等のような一般の事案であっても、デジタル・フォレンジックの対象となり得る。それらの事案に関連する人がパソコンやスマートフォン等の情報処理機器を使っていれば、その電磁的記録から関連する証拠を収集することができるからである[53]。

以下、インシデント発生後の対応として注目されているデジタル・フォレンジックの内容について整理する。

### 2－1　デジタル・フォレンジックとは

フォレンジック（forensics）は、もともと「法廷の」という意味のことばであり、英語では、「科学捜査」という意味で用いられることが多い。伝統的なフォレンジックのひとつとして「法医学」が挙げられる。法医学が医学と法学の連携・連鎖が必要であるように、デジタル・フォレンジック においては情報工学と情報法学の連携・連鎖が不可欠となる。特に最近は刑事分野に限らず民事分野や金融分野、医療分野などさまざまな領域へのデジタル・フォレンジックの利用が広がっており、学際化が進んでいる[54]。

デジタル・フォレンジックの定義は、明確に定まってはないが、警察庁では、犯罪の立証のための電磁的記録の解析技術及びその手続と定義し[55]、特定非営利活動法人デジタル・フォレンジック研究会では、インシデントレスポンスや法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連

53　安冨潔・上原哲太郎編著、特定非営利活動法人デジタル・フォレンジック研究会著（2019）『基礎から学ぶデジタル・フォレンジック　入門から実務での対応まで』日科技連出版社、1 頁。

54　須川賢洋「デジタル・フォレンジックの概論と新しい問題」（2021）『情報処理第 62 巻第 8 号』情報処理学会、オンライン版 el 頁。https://www.ipsj.or.jp/e-library/digital_library.html（2022.2.8 閲覧）

55　「用語集 デジタル・フォレンジック」警察庁 https://www.npa.go.jp/cyberpolice/words/index.html（2022.4.2 閲覧）

の科学的調査手法・技術と定義している[56]。

デジタル・フォレンジックが重要になってきた背景として、第1に、デジタル化の進展により、個人や組織の多くの情報交換が電磁的記録として保存・蓄積されるようになったため、捜査や民間での調査において電磁的記録が非常に重要なものとなっている。第2に、訴訟の増大があげられる。日本においても、国民の権利意識の増大などから、かつて想定されていなかった民事訴訟が行われるようになってきている[57]。このような状況から、裁判に対応するため、電磁的記録を電磁的記憶媒体から完全性を確保しつつ抽出し、証拠として訴訟に備えるための手順や技術が要求されるようになってきた。第3に、IoT化の進展などによりデジタルで扱う情報が膨大化し犯罪の増加と多様化が懸念されている。このような背景から、デジタル・フォレンジックはますます重要性を増していくと考えられる[58]。

デジタル・フォレンジックを分類する軸は多様であるが、ここでは特に訴訟の分類とデジタル・フォレンジックの対象に注目し整理する[59]。

①訴訟提起を受ける側としては、個人の場合と企業などの組織となる場合がある。②訴訟の対象行為としては、組織内の規則違反（個人）、組織間の契約などに違反、法律に違反（刑法など）の場合がある。③訴訟の種類としては、民事訴訟と刑事訴訟があり、④訴訟を提起する側としては、企業や個人、そして検察官の場合がある。

一方、デジタル・フォレンジックの対象としては、①サーバ、コンピュータ、ネットワーク（ルータ、ハブ、通信路等）、スマートフォン、IoT機器など証拠性の保持に関連する情報処理機器、②対象となるHDD（Hard Disk Drive）やSSD（Solid State Drive）などの電磁的記録を保管する媒体、③証拠の形態としてログや偶然残る痕跡、④情報システムの運用形態としてオンプレミス[60]やクラウドなどがある。

### 2－2　デジタル・フォレンジックの手順・内容

今日のデジタル社会の浸透によって、犯罪捜査は電磁的記録に頼らざるをえない状況にある。この電磁的記録は、誰でも容易に作成や削除、修正、改変、複写等ができる上、容量も膨大にな

56　中野目・四方・前掲注（15）121頁。「デジタル・フォレンジックとは」デジタル・フォレンジック研究会　https://digitalforensic.jp/home/what-df/（2022.4.2閲覧）

57　「基本的な統計資料」『弁護士白書　2021年版』日本弁護士連合会　https://www.nichibenren.or.jp/document/statistics/fundamental_statistics2021.html（2022.2.22閲覧）

58　安冨・上原・前掲注（53）3-4頁。

59　安冨・上原・前掲注（53）4-9頁。

60　サーバやソフトウェアなどの情報システムを、情報システムの使用者自身が管理する設備内に設置して運用すること。

る。そのため、電磁的記録を用いた犯罪捜査は、さまざまな技術を駆使しなければ適正かつ効率的な捜査ができない[61]。

デジタル・フォレンジック の大きな手順としては、①電磁的記録が保存されている電子計算機等の端末の収集または特定及び電磁的記録の保全、②当該電磁的記録データの検査、③記録データの分析（解析）、④解析結果報告書の作成がある[62]。

ここで、マルウェアに感染した被害端末を仮定すると、証拠保全は HDD・SSD の物理コピーとなる。コピー元の HDD・SSD に対しては、複写作業により動作記録等の追加書込みや書換えが行われないように書込防止装置等を用いて実施する。コピーが終了した後は、コピー元とコピー先のハッシュ値[63] を確認するが、このハッシュ値が一致せず、同一性を担保できない場合には、確認時の状況の写真撮影等を行い、同一性を担保する。

被害に遭った端末を特定し証拠収集及び証拠保全を行い、各種履歴等、痕跡データを解析して得られた結果から、サイバー犯罪に用いられた IP アドレスや接続されていた端末、悪用されたサービスのアカウント等を特定する作業を実施する。

近年では、多くの電磁的機器が、他の機器と連携するためにネットワークに接続されるようになってきており、リモートで接続可能な監視カメラやインターネットに接続可能なテレビ、あるいは HDD レコーダ機器など、IoT 機器に記録された電磁的記録も解析対象に含まれる場合がある[64]。

サイバー犯罪の被害に遭った端末を対象としてデジタル・フォレンジックを実施するが、当該端末に残存する痕跡データはサイバー犯罪全体の一部である。そのため、痕跡データを解析して得られた結果から被害実態を解明するための電磁的記録を収集する必要があるが、この作業は非常に困難なものである。

### 2 －3　証拠保全･犯罪者特定の難化

被害端末を証拠保全する際、不用意に端末を操作した場合には自動的に端末内の電磁的記録を

61　北條孝佳「サイバー犯罪とデジタル・フォレンジックの課題　―企業や組織における事前対策の備え―」（2021）『情報処理第 62 巻第 8 号』情報処理学会オンライン版、e8 頁。 https://www.ipsj.or.jp/e-library/digital_library.html（2022.2.8 閲覧）

62　北條・前掲注（61）e10 頁。

63　ハッシュ（Hash）値とは、「0」と「1」からなるデータを一定の法則で同じ長さに短縮した数値のこと。MD5（Message Digest 5）や SHA-1（Secure Hash Algorithm 1）などのハッシュ関数を使ってハッシュ値を求める。ハッシュ値の長さは一定（160 ビット）なので、同じハッシュ値になるように改ざんするのは困難であり、改ざん検知やファイルの同一性確認に役立つ。「ハッシュ」大塚商会 https://www.otsuka-shokai.co.jp/words/hash.html（2022.4.2 閲覧）

64　北條・前掲注（61）e12 頁。

消去するようなプログラムが、証拠隠滅のために犯罪者によって組み込まれている場合も考えられる[65]。

サイバー犯罪の被害を受けた端末の解析から、仮に接続元IPアドレスが特定できたとしても、接続元IPアドレスがTorの最後に経由するExitノードであった場合、Exitノードにアクセス履歴等が保存されるような機能が付加されていなければ、攻撃元を追跡することがきわめて困難となる。接続元IPアドレスが発展途上国のホスティングサーバであった場合、当該国の捜査機関と連携できない可能性があり、また、海外の匿名プロキシサーバが接続元IPアドレスであった場合には、当該プロキシサーバを利用した本来の接続元に関するアクセス履歴が存在しないため、攻撃元を辿ることはできなくなる。

日本国内であっても、公衆Wi-Fiや他人の居宅内に設置された無線LANのアクセスポイントから接続されていた場合には、攻撃元を辿ることが非常に困難となる。端末に痕跡が残らない海外のコミュニケーションサービスが使用されていれば、当該サービス提供事業者から接続元に関する履歴の提供を受けられなければ攻撃者を特定することが困難となり、また、Telegramのような秘匿性が高いメッセージアプリが使用されていた場合も同様である[66]。

サイバー犯罪が発生した場合に、どの端末やサービスがサイバー犯罪に使用されたか、あるいは被害に遭ったかを特定し、証拠保全のための準備をする必要がある。しかし、近年のマルウェアはファイルレスマルウェアとしてファイル自体が存在しないものも多く、マルウェア自体を抽出することができないこともある。また、マルウェアに感染した端末からファイル共有サーバに接続した履歴を保存していない環境であれば、接続履歴が存在しない。ファイル共有サーバにおいてファイルへのアクセス履歴すべてを取得していなければ、ファイル共有サーバから盗まれたデータを特定することもできない可能性がある。さらに、近年、企業が用いる端末はSSDが内蔵され、SSD全体が暗号化されているものが多いことも痕跡データが失われる原因の1つになっている[67]。

このように、証拠保全が実施されたとしても、被害実態を直接解明するための痕跡データがほとんど残っておらず、被害実態を解明するためには他の痕跡データから推定しなければならない場合も多い。さらに、デジタル・フォレンジックの作業を困難にしているのが、昨今のICT技術の革新によりセキュリティの向上が図られ、痕跡データが残らなくなっていることである。スマートフォンなどの端末はパスコードや指紋認証が必須になり、一定回数間違うと初期化され、端末内の電磁的記録を抽出できなくなる。端末内の電磁的記録全体に暗号化が施されていれば、削除された電磁的記録の復元さえもできなくなる。このような状況下はプライバシー保護のためには

65　北條・前掲注（61）e10頁。
66　北條・前掲注（61）e10頁。
67　北條・前掲注（61）e9頁。

有益であるが、犯罪被害の実態解明を困難にするという課題がある[68]。

近年、スマートフォン端末は、電子メールや画像データ、バックアップデータなど、ほぼすべての電磁的記録がクラウドサービスに保存されるようになってきているため、サイバー犯罪に関係するスマートフォン端末を特定し、当該端末を使用してどのようなサービスが使用され、クラウドサービスに保存されているかということが重要になる。

### 2－4　ファストフォレンジック

端末がサイバー犯罪の被害に遭った場合、被害申告のあった端末だけではなく、当該端末を経由して、他の端末がサイバー攻撃の被害を受けている可能性もある。そのため、迅速にすべての被害端末を特定し、被害全体を把握する作業が必要になる。

端末の操作ログをすべて保存するような EDR（Endpoint Detection and Response）[69] 等のシステムを導入していない企業や組織では、各端末から簡易的な情報を収集できるツール等を活用して、被害端末を特定することになるため、見逃しがあったり、重要な情報を収集できなかったりすることもある。このような作業は、非常に非効率的であり、時間だけが膨大に消費されてしまうため、ファストフォレンジックの実施が推奨されている[70]。ファストフォレンジックとは、早急な原因究明、侵入経路や不正な挙動を把握するため、必要最低限のデータを抽出及びコピーし、解析することをいう[71]。ファストフォレンジックを実施するには EDR の導入等、事前の環境構築や専用ツールの動作検証等の準備が重要になる。このようなファストフォレンジックを実施することによって、セキュリティ担当者の作業量の減少や被害の拡大を抑えることが可能となる。

## 3　デジタル・フォレンジックにおける法的な課題と対応策

本章ではデジタル・フォレンジックが利用された事件を概観した上で、法的な課題について整

---

68　北條・前掲注（61）e12 頁。

69　EDR が備える 4 大機能として、感染が疑われる異常な挙動を自動検出（検出）すること、不審な内部プロセスを停止・社内拡散や外部通信を遮断すること（封じ込め）、侵入に使われた脆弱性や経路・感染範囲を調査すること（調査）、マルウェアにより書き換えられたファイルなどの修復（修復）が挙げられる。「もう攻撃は防げない竹中工務店の大転換」（2020）『日経コンピュータ　2020 年 8 月 20 日号』日経 BP、23-26 頁。

70　北條・前掲注（61）e10 頁。

71　「ファストフォレンジックによる証拠データ抽出」『証拠保全ガイドライン 第 8 版』デジタル・フォレンジック研究会、36-37 頁。https://digitalforensic.jp/wp-content/uploads/2021/05/gl8-20210520.pdf（2022.4.2 閲覧）

理し、対応策について検討する。

### 3－1　事件・裁判におけるデジタル・フォレンジックの有用性

我が国の犯罪捜査におけるデジタル・フォレンジックの歴史は、平成 7（1995）年の一連のオウム真理教事件から始まった。信者の名簿が暗号化された記録媒体（フロッピーディスク）の解析を行い名簿について解読したことが黎明期のデジタル・フォレンジックであり、デジタル・フォレンジックの重要性が認識されるきっかけにもなった[72]。

また、平成 18（2006）年 1 月に発覚したライブドア社の有価証券報告書虚偽記載問題についての証券取引法（当時）等違反事件で、東京地検特捜部はサーバや端末として使われていたパソコンに対して徹底したデジタル・フォレンジック調査を行っている。サーバログの調査やデータリカバリにより、最終的には消去された電子メールを復元し、それをもって有罪の証拠とした。本件は、それまで主に凶悪犯罪事件の捜査のために使われていたデジタル・フォレンジックが、不正会計などの調査にも使われその有効性を示したという点で意味のある事件である[73]。

電磁的記録の改ざんが可能であり、また証拠として重大な影響を与えることが一般に認識された事件として、大阪地検特捜部検事によるフロッピーディスクの改ざん事件が挙げられる。障害者郵便割引制度の悪用事件に当時の厚生労働省の課長が関与したと疑われた事件において、フロッピーディスクのタイムスタンプが改ざんされた可能性が朝日新聞に特報[74]され、その日の夕方に主任検事が逮捕された。判決文（大阪地判平成 23 年 4 月 12 日判例タイムズ 1398 号 374 頁[75]）には、「高機能ファイル管理プログラムを用いてプロパティ情報を書き換え、さらに文書ファイルの順序を並び替えてもいる。その改変の態様は、特別の解析プログラムを用いることなしには改変の有無を判別することができないほど巧妙なもの」とある。検察の取調べ状況に合うようにタイムスタンプを書き換え、ファイルの並び順も変更した痕跡があった。担当検事にそのフロッピーディスクが渡る前の捜査報告書に記載されたプロパティ情報と、戻ってきた後のプロパティ情報が一致しないことから判明した[76]。

上記のほか、デジタル・フォレンジックを用いた解析結果に関する裁判例として下記のような

---

72　安冨・上原・前掲注（53）219-220 頁。「浦和フロッピーディスク差し押さえ事件特別抗告事件」（最判平成 10 年 5 月 9 日刑集第 52 巻 4 号 275 頁）参照。

73　安冨・上原・前掲注（53）221 頁。

74　「検事資料改ざん事件の特報、朝日新聞取材班に新聞協会賞」（朝日新聞デジタル 2010.10.6）http://www.asahi.com/special/kaizangiwaku/OSK201010060079.html（2022.4.2 閲覧）

75　現職の検察官が主任検事として担当する事件の証拠を改変したという証拠隠滅の事案につき、懲役 1 年 6 月の実刑判決が言い渡された事例。「大阪地検特捜部主任検事証拠改ざん事件」（2014）『判例タイムズ 1398 号』判例タイムズ社、374-376 頁。

76　安冨・上原・前掲注（53）223 頁。

事例がある。

岐阜地判平成23年1月28日（平成22年（わ）第276号・現住建造物等放火被告事件）では、住居兼神社に放火された事件につき、被告人の弁護人は、真犯人は別人として放火の事実を争ったが、裁判所は、被告人が使用していたパソコンのインターネット閲覧履歴、被告人電子メールの内容から、犯人であることが強く推認され、上申書、弁解録取書の内容が信用できることも併せ考慮すると、被告人が犯人であるとした[77]。

つづいて、金沢地判平成24年3月2日（平成23年（わ）第70号・強盗殺人、死体遺棄被告事件）は、債務を負っていた被告人が相手方である被害女性を殺害し死体を遺棄したという事件である。裁判所は、犯行当日後の被告人方のパソコンの「白骨化」「海岸 白骨」等のインターネット検索履歴、捜査官作成の「パーソナルコンピュータの解析結果について」と題する書面、被害者と第三者の間でなされた携帯電話のメール内容等の証拠から、被告人が犯人でなければ、説明することが極めて困難な事実があるといえると指摘した[78]。

上記の判決では、いずれもインターネネット閲覧履歴などについて、被告人が犯人であることを推認する間接事実として積極的に評価している。

デジタル・フォレンジックを用いた解析結果から犯罪事実を認定するにあたっては、保全された電磁的記録媒体には膨大な電磁的記録が記録されているが、「どのような電磁的記録を用いて要証事実を認定するか」は慎重に検討することが求められる。デジタル・フォレンジックによる解析結果は、「検察官が主張する起訴状に記載された犯罪事実を立証できるか」について、刑事訴訟上問題となるすべての事実が証明の対象となるとして法的な観点から厳格に吟味する必要がある[79]。

### 3－2　デジタル・フォレンジックの法的論点

本節では、デジタル・フォレンジックにおける法的な論点について整理する。

デジタル・フォレンジックに直接関連する論点として、まず第1に、デジタル情報をすべて証拠として使うことができるかという問題がある。デジタル情報は改ざんが容易であるため、電磁的記録が証拠として提出されても、それが真正なものだという確信が持てない場合が多い。そこで実務では、デジタル・フォレンジック技術を用いて内容が改変されていないことを確認できるようにすることが行われる[80]。

刑事訴訟法では、証拠能力の有無が条文に規定されており、供述証拠については、反対尋問な

77　安冨・上原・前掲注（53）152頁。
78　安冨・上原・前掲注（53）152-153頁。
79　安冨・上原・前掲注（53）155-156頁。

ど一定の条件を満たさなければ証拠能力が否定されることがある。しかし、現行の刑事訴訟法上の規定では、デジタル情報の真正性を確保するための措置が行われていない場合でも、その情報の証拠能力が否定されることはない。民事訴訟法においては、証拠能力を制限する規定は設けられていない。証拠として提出された文書が真正か否かについては、提出した者が証明しなければならないが、正規の手続で作成された公文書や署名押印のある私文書は、反証がなければ真正なものと扱われる[81]。

第 2 に、デジタル・フォレンジック技術による措置の有無が、裁判官の判断にどの程度影響するかという問題がある。刑事訴訟（刑事訴訟法第 318 条）や民事訴訟（民事訴訟法第 247 条）では、証拠に基づく事実認定について裁判官の自由心証主義が採られている。したがって、どの証拠をどの程度重視して判断するかは、原則として裁判官の裁量に委ねられている。先述（3－1）のとおり、最近ではデジタル・フォレンジック技術を利用した適切な保全が行われているかどうかが、裁判の帰結を左右する場面も出てきている。

民事訴訟は対等な当事者同士が争うことになるが、捜査機関と被疑者が争う刑事訴訟においては、立場が対等ではないため、被告人側が捜査機関の提出した証拠の真正性を争うことは非常に困難である。証拠の真正を問う場合、刑事訴訟の実務では被告人の不利益があると考えられる。一般に、捜査機関側による証拠のねつ造はないという暗黙の了解のもとに裁判が進められていた。しかし、平成 22（2010）年 10 月に起きた先述の大阪地検証拠（フロッピーディスク）改ざん事件において、捜査機関によるデジタル証拠のねつ造が明らかとなり、捜査機関の信頼性が失われた[82]。これらのことから、捜査機関の証拠を判断する裁判所において、電磁的記録の真正性ついてどのような措置が行われているのかを勘案して証拠を取り扱うことが求められる。

第 3 に、デジタル・フォレンジック技術を利用することが法的に許されるかということが問題となる。これは、憲法や電気通信事業法上の秘密やプライバシー侵害等に関する問題である。刑事訴訟においては、新たな技術によって強制処分に当たる捜査が行われた場合、どのような範囲で許容されるか問われることになる。例えば、写真・ビデオ撮影、体液の採取、通信傍受等については、捜査機関がどのような方法で証拠を採取することが許されるのかが議論されている。捜査当局は、犯罪が発生した際にさまざまな方法で手がかりを探し、新技術によって生成されたデー

---

80　小向太郎「デジタル・フォレンジックとこれからの法律研究」（2021）『情報処理第 62 巻第 8 号』情報処理学会　オンライン版、e13 頁。https://www.ipsj.or.jp/e-library/digital_library.html（2022.2.8 閲覧）

81　民事訴訟法 228 条 1 項「文書は、その成立が真正であることを証明しなければならない」2 項「文書は、その方式及び趣旨により公務員が職務上作成したものと認めるべきときは、真正に成立した公文書と推定する」4 項「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する」。小向・前掲注（80）e13-e14 頁。

82　小向・前掲注（80）e14 頁。

タも含めて、犯罪に少しでも関係する可能性のある人物の情報を収集している[83]。最近では、AIによる個人分析や個人のデータプロファイリングについて、人権を脅かす可能性があるとして疑念が示されるようになっている[84]。犯罪捜査への利用についても、冤罪や被疑者の差別的な取り扱いに繋がる可能性がある。デジタル・フォレンジック技術の利用によって、個人のプライバシーにかかわる事実が明らかになる場合も多いため、プライバシー保護の観点からの検討が重要になる。

例えば、現在では犯罪捜査のために監視カメラやドライブレコーダで録画された映像や、メールやSNS、ネットサービスの利用履歴、位置情報、アクセスログなどの情報システムにある個人の痕跡を利用している。これらの個人の情報を照合して、罪を犯す可能性のある人物のリストや行動履歴を作成し容疑者を特定することで、犯罪捜査の効率化を図ることができる可能性もある。

また、捜査機関が、被疑者等の当事者ではなく、第三者から情報収集することも増えている[85]。我が国の犯罪捜査においては、人権の侵害や制約を伴う強制処分をできる限り回避するべきであるという考えから任意捜査の原則が採用されている[86]。本人の意思に反して個人情報を取得することは強制処分ともいえるが、捜査当局が個人情報を保有する第三者に情報を求めることは一般的には強制的な処分ではないと考えられており、強制捜査として令状の取得等がなくても行うことができる[87]。例えば、個人情報保護法は、個人情報取扱事業者が本人から事前の同意を得ずに個人データを第三者に提供することを原則として禁止しているが、捜査機関が捜査の目的で提供を求める場合には、「法令に基づく場合（改正法27条1項1号）」として本人の同意がなくとも提供ができると考えられている。

令和3（2021）年の改正（「デジタル社会の形成を図るための関係法律の整備に関する法律」2021年5月成立）によって、我が国の個人情報保護に関する法律は、個人情報保護法に統合され、地方公共団体の個人情報保護制度についても統合後の法律において全国的な共通ルールを規定し、全体の所管が個人情報保護委員会に一元化されることになった。これによって捜査機関も個人情報保護委員会の監督を受けることとなったが、犯罪捜査等に関する情報は適用が除外される場合

83　サイバー犯罪では、犯罪現場が実際に存在している従来の犯罪者プロファイリングでは対応できない。そこで、計量的文体分析の手法（テキストマイニング）を用いて、印字された文書、電子メール、電子掲示板など文章情報にもとづき著者の特徴を推定する著者プロファイリングが求められる。財津亘（2019）『犯罪捜査のためのテキストマイニング』共立出版、155-156頁。

84　小向・前掲注（80）e14頁。笹倉宏紀「AIと刑事法」（2018）山本龍彦編著『AIと憲法』日本経済新聞社、394頁以下。

85　小向太郎「捜査機関による第三者保有の個人情報に対するアクセスと本人の保護」（2020）『情報通信政策研究』第4巻第1号総務省情報通信政策研究所 、63頁以下。https://www.jstage.jst.go.jp/article/jicp/4/1/4_63/_pdf/-char/ja（2022.3.21閲覧）

86　犯罪捜査規範第99条「捜査は、なるべく任意捜査の方法によって行わなければならない」。

87　小向・前掲注（80）e15頁。

が多いと考えられる（改正法 74 条など）。しかし、個人情報保護制度は、もともと情報技術の発達で膨大な量の情報が収集・保存されることによる危険や弊害に対処するために整備されてきたものである。我が国の犯罪捜査を含む法執行機関の活動における個人情報の取扱いについても、一定の規律や透明性の確保が求められる[88]。

デジタル・フォレンジックにおいて証拠保全を行う場合、先述したように保全対象となる HDD・SDD 全体をコピーすることになる。この作業は物理コピーとも呼ばれ、対象となる端末の HDD・SSD にインストールされた OS やプログラム等もコピーすることになる。この際、著作権との関係が問題になる。例えば、被害に遭った HDD・SSD の OS やプログラム等について、被害当時の状況を保全するためにコピーし、第三者に調査解析を行わせるなどの場合、プログラムの実行等によってその機能を享受することに向けられた利用行為ではないと評価できるため、著作権法 30 条の 4（著作物に表現された思想または感情の享受を目的としない利用）に該当し、著作権侵害には該当しないと考えられる[89]。

近時施行された令和 4（2022）年改正警察法では、国家公安委員会及び警察庁の犯罪捜査を認められることになったことが挙げられる。国の機関である国家公安委員会及び警察庁はこれまで、これまで事務を行う行政機関、都道府県警の総合調整機能のみを有し、自らが犯罪捜査を行うことを認められていなかった。なぜならば、かつての特別高等警察のような思想や言論、行動を取り締まることを専門にした中央集権的な国家警察が否定され、戦後改革によって地方警察が警察活動を行うこととしたことに由来している。しかし、今回の改正警察法で犯罪捜査を認められたことは、中央集権的な国家警察の復活との批判が向けられている[90]。デジタル・フォレンジックの利用についても、個人の思想やプライバシー保護、そして、著作権などさまざまな観点から慎重に取り扱う必要があると考える。

---

88　小向・前掲注（80）e15 頁。法執行機関による個人情報へのアクセスについては、日本と EU の間の相互の個人データ移転枠組み構築に関する取り組みの過程でも議論になっている。日本と EU の間では、相互に個人情報保護が十分な国と認める方向で検討が行われ、平成 31（2019）年 1 月 23 日には、欧州委員会が、日本に対する十分性を認める決定をしている。その過程で、欧州委員会から日本政府による情報のアクセスについて説明が求められ、法務省が、欧州委員会の Věra Jourová 委員（司法・消費者・男女平等担当）に、概要を説明する書簡を送付している（個人情報保護委員会「日 EU 間・日英間のデータ越境移転について」個人情報保護委員会（PPC） https://www.ppc.go.jp/enforcement/cooperation/cooperation/sougoninshou/（2022.3.22 閲覧）

89　北條・前掲注（61）e10 頁。

90　「4 月発足　サイバー警察局に学者ら懸念の声　警察庁初の直接捜査に戦後警察の骨格変わる」『東京新聞 2022.4.1』https://www.tokyo-np.co.jp/article/169026（2022.4.2 閲覧）。

## おわりに

以下に、本稿で検討した内容を整理したい。

まず第1に、サイバー犯罪では、記録媒体の電磁的記録の特性とインターネット上の匿名性という大きな特徴が悪意をもって利用されていることがあらためて確認された。また、リモートワークで用いられるVPN機器の脆弱性等が狙われる場合や、国際紛争のなかで国家を背景に持つサイバー攻撃集団によるサイバー攻撃が明らかになるなど、サイバー空間をめぐる極めて深刻な情勢が拡大している。このような深刻な状況に対応するため改正警察法が令和4（2022）年4月1日から施行され、サイバー警察局や全国を管轄する特別捜査隊を関東管区警察局に設置されるなど重大な局面を迎えることになった。

第2に、サイバー犯罪に関わるインシデントが発生した場合、電子的記録の保存・解析を行い裁判に備えるための証拠保全を行う一連の科学的調査手法・技術としてデジタル・フォレンジックに焦点を当て、技術的な側面の手続きと技術的課題について整理した。デジタル・フォレンジックには情報技術に関する高度な専門性を要する。しかし、近時増加しているランサムウェアを用いたサイバー空間の犯罪者等は、電磁的記録に痕跡データが残らないような高度な技術力を用いて攻撃を行う場合が多い。したがって、常に解析技術の更新が必要となることが明らかとなった。また、電子端末におけるプライバシー保護のためのICT技術の進展が、同時に痕跡データの追跡を困難にし、犯罪被害の実態解明を困難にしてしまうという課題も見出された。

第3に、我が国の犯罪捜査におけるデジタル・フォレンジックの歴史は25年を越えているが、これまでの事件や裁判を振りかえると、証拠として提出される電磁的記録の真正性を確保できるのかという課題があることが明らかとなった。裁判官の自由心証主義が採られている訴訟にあっては、デジタル・フォレンジックの証拠能力について、原則として裁判官の裁量に委ねられることになる。高度な学際的知見を要するデジタル・フォレンジックについては、裁判官においてもその技術的背景の基本的理解を深めておく必要がある。なぜならば、裁判官の技術的理解の程度によって結果に大きなばらつきが生じることが考えられるからである。特に刑事訴訟の場合のように、被告人側が捜査機関の提出した証拠の真正性を争う場合は、立場が対等でないため特に注意が必要である。捜査機関によるデジタル証拠のねつ造があったことを記憶しておく必要がある。

最後に、デジタル・フォレンジックにおいて、個人のデータプロファイリングを行う過程でプライバシー権や著作権などへの関係が課題となっている。現状では、捜査機関も個人情報保護委員会の監督を受けるが、犯罪捜査等に関する情報は適用が除外される場合が多い。また、捜査機関による物理コピーはプログラムの実行等によってその機能を享受することに向けられた利用行為ではないと評価できるため、著作物からの享受を目的としないと解され、著作権侵害には該当

しないと考えられている。しかし、改正警察法におけるサイバー警察局の設置や特別捜査隊の設置は、捜査機関の権限を拡大するものであるため、今後注視していく必要があると考える。

**参考文献等**

秋山満昭・島岡政基「サイバーセキュリティ研究における心理的配慮のサポート」（2020）『情報処理第 61 巻第 4 号』情報処理学会、378-383 頁

石黒正輝・新誠一・佐々木貴之「新たなモビリティ時代のサイバーセキュリティ」（2020）『情報処理第 61 巻第 4 号』情報処理学会、330-331 頁

板倉陽一郎「ドコモ口座はなぜ攻撃されたか？～開設時本人確認と出金時本人確認の間隙～」（2021）『情報処理第 62 巻第 7 号』情報処理学会、336-339 頁

上原哲太郎「最新のデジタル・フォレンジックにおける技術的課題」（2021）『情報処理第 62 巻第 8 号』情報処理学会オンライン版、e4-e7 頁 https://www.ipsj.or.jp/e-library/digital_library.html（2022.2.8 閲覧）

垣内秀介「発信者情報開示手続きの今後」（2021）『ジュリスト＃ 1554』有斐閣、25-31 頁

北澤一樹「名誉棄損（信用棄損）に当たる誹謗中傷とは」（2021）『ジュリスト＃ 1554』有斐閣、31-37 頁

實原隆志「個人情報の定義等の統一」（2021）『ジュリスト＃ 1561』有斐閣、34-39 頁

須田守「行政手続のデジタル化と法的課題」（2021）『ジュリスト＃ 1556』有斐閣、19-24 頁

高橋郁夫他編（2015）『デジタル証拠の法律実務 Q&A』日本加除出版

寺川永「消費者契約法と事業者的消費者」（2021）『ジュリスト＃ 1558』有斐閣、16-21 頁

中川丈久「デジタルプラットフォームと消費者取引」（2021）『ジュリスト＃ 1558』有斐閣、40-46 頁

西貝吉晃（2020）『サイバーセキュリティと刑法 - 無権限アクセス罪を中心に』有斐閣

林優一・川村信一「ハードウェア電子機器トロ―ジャンの脅威と検出」（2020）『情報処理第 61 巻第 6 号』情報処理学会、558-571 頁

本間尚文・上野嶺「ハードウェア電子機器に対する物理攻撃―サイバーだけでなくフィジカルも守る」（2020）『情報処理第 61 巻第 6 号』情報処理学会、560-563 頁

「守り切れない時代のクライアントセキュリティ」（2020）『日経コンピュータ　8 月 20 日号』日経 BP、22-35 頁

町村泰貴・白井幸夫編（2016）『電子証拠の理論と実務―収集・保全・立証』民事法研究会

松原豊・倉地亮・高田広章「自動車分野の CASE 革命とサイバーセキュリティ」（2020）『情報処理第 61 巻第 4 号』情報処理学会、338-343 頁

丸橋透「媒介者の責任―責任制限法制の変容」（2021）『ジュリスト＃ 1554』有斐閣、19-24 頁

安冨潔「ユビキタス社会におけるサイバー犯罪：情報セキュリティの保護法益」（2008）『慶應の法律学刑事法：慶應義塾創立一五〇年記念法学部論文集』慶應義塾大学法学部、281-306 頁

渡邊卓也（2018）『ネットワーク犯罪と刑法理論』成文堂

外務省（2021）「サイバー行動に適用される国際法に関する日本政府の基本的な立場」https://www.mofa.go.jp/mofaj/files/100200951.pdf（2022.2.22 閲覧）

経済産業省（2021）「特定デジタルプラットフォームの透明性及び公正性の向上に関する法律案の概要」https://www.meti.go.jp/press/2019/02/20200218001/20200218001-1.pdf（2022.2.2 閲覧）

総務省（2020）「SNS 上での誹謗中傷への対策に関する取組の大枠について」https://www.soumu.go.jp/main_content/000695577.pdf（2022.2.2 閲覧）

法務省（2021）「第 4 編各種犯罪の動向と各種犯罪者の処遇　第 4 章サイバー犯罪」『令和 2 年版犯罪白書―薬物犯罪―』https://www.moj.go.jp/content/001363987.pdf（2022.2.22 閲覧）

法務省（2022）「第 4 編各種犯罪の動向と各種犯罪者の処遇　第 5 章サイバー犯罪」『令和 3 年版犯罪白書―詐欺事犯者の実態と処遇―』96 頁 https://www.moj.go.jp/content/001365724.pdf（2022.2.22 閲覧）